DEPARTMENT OF THE ARMY
SAVANNAH DISTRICT, CORPS OF ENGINEERS
CESAS-IM P.O. BOX 889
SAVANNAH, GEORGIA 31402-0889

DISTRICT PAMPHLET 24 Jul 03
NO. 25-1-13

## Information Management
## COMPUTER–USER SECURITY GUIDE

1. This change to DP 25-1-13, 9 Dec 2002, is issued to correct Appendix C.

2. Substitute the enclosed pages as shown below:

| Remove Pages | Insert Pages |
|---|---|
| C-1 | C-1 |

3. File this sheet in front of the publication for reference purposes.

/s/
Encl ROGER A. GERBER
COL, EN
Commanding

CESAS-IM 9 Dec 02

MEMORANDUM FOR DISTRIBUTION F

SUBJECT: Comp uter-User Security Guide

1. Each day we become more and more information dependent. It is therefore necessary to ensure that all precautions are taken to protect our information systems from unauthorized access.

2. It is mandated by Department of the Army DOD Directive 5200.40, DOD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 Dec 97, that all computers and information systems be accredited and certified.

3. One of the requirements is to ensure all team members are educated on computer security. The enclosed pamphlet provides the necessary information on topics such as securing passwords, ensuring anti-virus software is running on computers, and the points-of-contact to report suspicious activity.

4. Team members are strongly encouraged to take the computer security self-assessment test after reading this pamphlet. This will provide a means of gauging knowledge and comprehension on the importance of security such as the proper notification process if passwords are compromised, software and hardware installation guidance, and authorized web sites.

5. Computer security is an integral key to network continuity of operations and protection of information in accordance with AR 380-19, Computer Systems Security, 27 Feb 98. It is our responsibility to take all necessary precautions to protect our computers and systems in order to carry out our mission.

/s/

Encl

ROGER A. GERBER
COL, EN
Commanding

US Army Corps
of Engineers
Savannah District

## U.S. Army Corps of Engineers

# DISTRICT PAMPHLET 25-1-13

# Information Management

# Computer-User Security Guide

**9 December 2002**

**This Pamphlet supersedes DP 25-1-13, 19 July 2001.**

# TABLE OF CONTENTS

APPENDICES

1. Purpose. This pamphlet is a guide to using Government computers in the workplace. In support of information assurance, this guide prescribes procedures for using computers in a way that protects them against viruses and hackers. This guide is your driver's manual for the Infobahn. Before you can be issued a license to "drive," you must read this guide and sign the User Agreement upon issuance of your passwords from the UPASS Administrator

2. Applicability. This pamphlet applies to all U.S. Army Corps of Engineers, Savannah District, military and civilian personnel who use Government computers in the workplace.

3. References.

a. AR 380-19, Computer Systems Security, 27 Feb 98.

b. AR 380-53, Information Systems Security Monitoring, 29 Apr 98.

c. DOD Directive 5200.1-R, Information Security Program, Jan 97.

d. DOD Directive 5200-28, Security Requirement for Automated Information Systems (AISs), 21 Mar 88.

e. DOD Directive 5200.40, DOD Information Technology Security Certification and Accreditation Process (DITSCAP), 30 Dec 97.

f. DOD 5500.7-R, Joint Ethics Regulations, Aug 93.

4. General. The proponent of this guide is the Information Assurance Security Officer (IASO), Kerry Taylor, 912-652-5861. Suggested improvements to this guide can be made by sending an e-mail to Kerry Taylor.

5. Introduction. As a U.S. Army Corps of Engineers, Savannah District computer user, your actions can greatly increase or decrease the integrity, availability, and confidentiality of information concerning national defense. Protecting that information is called "information assurance." This guide will help you understand and enforce information assurance by showing you how to recognize and avoid the hazards awaiting you once you enter the "Infobahn." This guide is your drivers manual for the Infobahn.

6. Your Computer as a Gateway to Information.

a. Since almost all unclassified U.S. Army Corps of Engineers, Savannah District computers are networked, your computer has access either through your local area network (LAN) or over the Internet to almost every unclassified computer in the entire Department of Defense (DOD). This internetworking of computers makes your computer a gateway to vast amounts of sensitive but unclassified information. The security of our networks is only as strong as the weakest link. As a user of a computer within Savannah District, you play a key role in ensuring the availability, confidentiality, and integrity of our data. Comply with the rules that follow, and you will not be the weakest link.

b. If you can get out, a hacker can get in. A basic premise of networked computing is that if you have access to the Internet through your computer, hackers have access to you. Remember, the Infobahn is a two-way street.

c. Since your computer is "trusted" by other computers within the military domain, it provides access to various military networks. "Trusted" means that other computers recognize your computer as a Department of the Army computer. As such, you can obtain passwords and gain access to certain information not available to non-military users. Based on that, your actions can put your computer, your unit's network, and all Army computer networks at risk. Your use of a Government computer therefore places a great deal of responsibility on your shoulders. You are directly responsible (along with others) for the security of the Army's computer networks.

7. Local Area Network and Internet Connectivity. The Local Area Network (LAN) is a data network created for the U.S. Army Corps of Engineers, Savannah District, that is intended for transmission of only unclassified information. We use the LAN to communicate worldwide. The LAN is linked to the World Wide Web (the Internet). We therefore need to know who has access to the LAN to protect ourselves against hackers. This is why we cannot allow users to create "backdoors" to the Internet through the LAN. A "backdoor" is an unauthorized, unknown connection between the LAN and the Internet. If, for instance, your computer is connected to the network through a LAN, simultaneously connecting to the Internet through a modem to a commercial Internet service provider creates a backdoor, which is prohibited.

8. How to Treat Your Computer.

a. Your computer is an important part of the toolkit you need to do your job. You therefore must treat your computer with care. Heat is your computer's worst environmental enemy. Exposing your computer to heat will shorten its lifespan and put your data at risk. Take care not to expose computers to portable heaters.

b. Do not eat or drink near your computer. Spilling soft drinks, coffee, or other liquids on your computer can damage it and destroy your files.

c. Keep your system clean and free of dust.

d. Do not disconnect your computer from its network. The small network connections are very fragile and very expensive.

e. Do not move your computer. This needs to be coordinated through LM and IM. Most damage done to computers occurs while moving them. Computers also wind up missing after moves; so care must be taken to notify the hand-receipt holder of the computer's new location.

f. Turn your computer off at the end of the day. If your computer is turned off, it cannot be hacked. This also reduces the chance of a fire and does not waste electricity.

g. When computers are unattended, logoff or ensure your computer is set with an automatic password screen saver. The HelpDesk can assist you with the configurations.

h. In many ways, you as a user can cause the biggest threats to your computer. Take care of your computer by following the above instructions and your computer will perform its many valuable functions for you day after day.

9. Personal Use of Your Government Computer.

a. We have detailed rules for appropriate and inappropriate use of Government computers. We also have rules governing how you may use your Government computer for personal use. The U.S. Government provides you a computer to do your assigned duties. Government computers may be used only by Government employees for the following:

(1) Official business (paragraph b below).

(2) Authorized personal use (paragraph c below)

b. Official business is that which is related to your official duties.

c. Authorized personal use is defined in the Joint Ethics Regulation (JER). Authorized personal use includes brief access and searches for information on the Internet and sending short e-mail messages.

d. The JER also requires commanders and supervisors to make every effort to ensure that personal use of Government computers--

(1) Does not adversely affect the performance of official duties.

(2) Is limited to reasonable durations and frequency and, when possible, done during off-duty hours.

(3) Serves a legitimate public interest, such as furthering the education and self-improvement of employees.

e. Personal use of Government computers must not overburden the communication system. Remember, here at the U.S. Army Corps of Engineers, Savannah District, the communication system is designed to support our missions.

f. Personal use of Government computers must not reflect adversely on DOD or DOD components. The JER specifically prohibits using Government computers for pornography, chain mail, personal gain, or any action that violates another statute or regulation.

g. Other misuse of Government computers includes hacking or using hacker tools, visiting hacker websites, deliberately installing viruses on DOD computers, trying to mask or hide your identity, attempting to bypass security policy, and using Internet telephony, "streaming" audio/video websites (for example, keeping a webpage open to receive hourly stock updates).

h. Misuse of Government computers is subject to reprimand.

10. The Importance of Passwords.

a. Your password is the key that gets you onto the information highway. While this key opens the vast world of various military networks and the Internet, it can also allow others access to the same information. Maintaining the security of your password is one of the most important security precautions you have as a user. Therefore, password security is VERY important.

b. The security of your password is important to maintaining the integrity of our networks. If your password is compromised, a computer intruder can access all data to which you have access. You should not write down your password, nor should you ever share your password with anyone. Also, do not store your login IDs and passwords on any electronic media (i.e., floppy disks, CD-ROM) and/or store as a file on your computer or the network. If someone obtains and uses your password, they could become "you" in the virtual world. You are responsible for anything that occurs on the network under your log-on name and password. If you share your password and someone logs on as you and then hacks a website or downloads a hacker tool, you could be held responsible.

c. Passwords will be locked in a secured environment. Passwords will not be taped, stored, or written on computers, keyboards, monitors, etc.

d. As a computer user in Savannah District, you will have a unique log-on name and password for each computer account you use. AR 380-19 requires passwords to be at least eight digits long, include at least two numbers, and not form a word. You may not tamper with your computer to avoid the password policy.

e. Passwords that do not conform to the standard eight-alphanumeric configuration are very vulnerable to password-cracking programs continually used by hackers. Most cracker programs compare passwords to words in dictionaries. If your password is made up of words or acronyms, the program unscrambles your password and gives the hacker access to your computer. Once hackers gain access to your computer, they have access to much of the DOD network. Password protection is essential.

11. Viruses.

a. Computer viruses are programs that corrupt and damage programs and data. A program does not have to perform malicious actions to be a virus; it only needs to infect other programs. Almost all viruses, however, perform malicious actions. Deliberately introducing "malicious logic" (the technical term for viruses and other malicious programs) into any Government information system is a Federal crime for any soldier, DOD employee or contractor. Withholding information needed to effectively implement countermeasures or antivirus protection is also against the law.

b. How do viruses get into your computer? Viruses can invade a system through any normal means of communicating, transferring, or sharing information (for example, through diskettes, CD-ROMs, modems, network interfaces, communication ports). The most common means of spreading a virus is through e-mail. Viruses that are spread through e-mail are inserted into files, which are sent as e-mail attachments. Remember that the virus is not in the body of the e-mail; it is in the attachment. Opening the attachment releases the virus. This is the most common method of spreading new viruses; users therefore need to be very careful when receiving e-mail attachments. Some viruses compromise the confidentiality of data and clog the e-mail system, hindering the availability of data. Other viruses use personal address books to spread. When, for example, a user opens an infected e-mail attachment, the virus sends the attachment to the first 50 addresses in the user's address book. More recent and more destructive viruses erase a variety of files, including Word documents, Excel spreadsheets, and PowerPoint slides.

c. Many macro viruses exist. They are written for Word macro language and are spread through Word documents. This is a very serious problem, since we exchange so many Word documents by e-mail; as soon as the attached document is opened, the virus is activated. The more creative macro viruses use your personal address book or in-box to rapidly spread the virus by e-mail. The Melissa virus was spread worldwide in a matter of days. The speed at which new viruses can be spread by e-mail can cripple an entire e-mail system by generating more messages than the system can handle. If you receive an e-mail message with a suspicious attachment, delete or scan the attachment for viruses before opening it. If you are still concerned, do not open the attachment; instead, contact the IASO.

12. Detecting and Preventing Viruses.

a. The best course of action is to prevent viruses from infecting your computer in the first place. Here are some things you can do:

(1) Use the current, DOD-authorized version of antivirus software. Savannah District uses Norton Anti-Virus software as the standard. Savannah District's policy requires you to update your computer's antivirus software once a week. Currently, this is done automatically when you log on your computer. You will be notified when the software has been updated and instructed to reboot your computer for the new system changes to be in effect. Remember, those who create antivirus software are always one step behind those who are creating new viruses. Ensure the antivirus software application is running. If you are unsure, contact the Helpdesk at 912-652-5946.

b. Even when taking the best precautions, viruses can still occur. They are not always immediately identifiable. Here are some things that may indicate the presence of a virus:

(1) Abnormal displays or banners.

(2) Your computer's performance slows down.

(3) Unusual activity, error messages, changes in file sizes, and loss of programs or data.

c. The above symptoms do not always mean that your computer has a virus. You need to be aware, however, of these abnormalities and report them to the IASO as soon as they occur.

d. Diligent use of antivirus software by all users of Government computers is the best way to prevent damage to Savannah District's networks and data by viruses. Antivirus software companies are constantly updating their product. If you, as a computer user, keep your antivirus software running and up-to-date, your chances of getting a virus are very low. If every user at Savannah District kept their antivirus software up-to-date, and running, the number of viruses would drop dramatically. By keeping your antivirus software up-to-date and running, you will most likely never suffer the problems caused by viruses.

e. If you find a virus, contact the Helpdesk immediately. Prompt reporting of viruses can lessen their effect by giving security officers time to warn coworkers, who can then check their computers for the virus. If you have a new virus, chances are good that others in your organization will have the same virus. If your system is infected, first make sure you have the most current version of antivirus software. Then disinfect all files. If you are unsure how to use the antivirus software, the Helpdesk can provide assistance. Improper use of the software may fail to find all viruses. Do NOT open any attachments. The Helpdesk can clean the virus and lessen the chance of further spreading the virus. Always re-scan to make sure all viruses have been eliminated. We will never be completely free of viruses, but with the correct measures, we can do a better job of controlling them. Ensure your antivirus is running, scan all diskettes, and be sure not to open suspicious e-mail attachments.

13. Chain-Mail, Virus Hoaxes, and Other Computer Hoaxes.

a. The Internet is constantly flooded with bogus information (for example, messages about potentially damaging viruses, notices that Bill Gates will send you money for forwarding e-mail to others). While some real information may be mixed in with these hoaxes and urban legends, it is unlikely. The best course of action on receipt of these types of messages is to delete them without reading them. The premise behind a hoax is that it will stimulate the reader to get emotionally involved (for example, by making the reader angry, afraid, eager for money offered) and immediately forward the message to everyone the reader knows or can reach through a Global Address List. That creates "chain-mail," which in turn creates bottlenecks of electrons in our e-mail and other network servers, slowing them down. Chain mail can even cause network servers to "crash." Because of this threat to our systems, you are strictly forbidden from forwarding hoax messages to anyone except the IASO.

b. Virus hoaxes are not real viruses, but they can be harder to get rid of than real viruses. Virus hoaxes and other e-mail hoaxes take up space on e-mail servers, use up network bandwidth, and waste time. Virus hoaxes are more common (and sometimes more timeconsuming) than actual viruses. They usually take the form of e-mail warnings sent to large numbers of people to warn them about nonexistent viruses.

c. If you receive a warning and are not sure if it is real, do not send it to everyone you know; forward it your IASO. Here are some common hoaxes:

(1) Telephone Scam-Request to Forward

(2) Join the Crew

(3) Pen pal Hoax

(4) AIDS Hoax

(5) Bill Gates $1000 chain mail

(6) Win-a-Holiday

(7) BUDDYLST.ZIP

d. When any of the items above are forwarded to large numbers of users, they use up bandwidth, take up space on e-mail servers, and mislead recipients. Forwarding chain-mail hoaxes violate the JER and Army policy. Data networks were designed to support the missions at the U.S. Army Corps of Engineers; forwarding chain mail does just the opposite by causing systems to overload and fail, thus blocking our ability to communicate.

14. Use of Hardware and Software.

a. Software. Software used on Government computers must be licensed, accredited, and approved by Information Management Office. If you want to load private software on your Government computer, you must have the approval of the IASO or Information Assurance Manager (IAM). You may not load any games or shareware programs on your computer. All software on your computer must meet standards established by the Information Management Office. Original disks and/or official software license must accompany each computer and be used in accordance with the licensing agreement.

b. Hardware. Any Government supplied hardware you use or purchase must be accredited and approved by Information Management Office. As the user, you must maintain property accountability. You cannot install and use your own hardware at work.

15. Reporting Computer-Security Incidents.

a. Users must report any suspected individual computer-security incidents to the IASO or, in the absence of the IASO, to the IAM. IASOs report to IAMs.

b. Users must report all network-security incidents to their IASO. If you think you observed a network-security incident, report it to your IASO and let the IASO determine whether or not it requires further investigation.

c. Users are often the first in the command to recognize a new virus. Reporting viruses to your IASO or IAM as soon as you detect it will greatly increase the chances of catching and stopping the virus from spreading any further.

d. Users are also among the first to notice intrusions by hackers. Some indications of a possible intrusion are seeing a web-browser open on your screen without your having opened it, noticing your CD-ROM drive trying to read a compact disk (CD) without your prompting it, or finding that your files are mysteriously being deleted or moved. If any of these things are happening, you may be the victim of a hacker and must report the incident to the IAM or IASO immediately.

16. Monitoring. Your use of a Government computer constitutes consent to monitoring. When you click OK on the warning banner, which opens when you start your computer, you are giving your consent to having your computer monitored. Your Government computer is provided to you for authorized use only. Government computers are monitored to ensure that use is authorized and that users follow security procedures. Monitoring is also done to see if hackers have gained access to computers. Privacy does not exist on Government computers therefore users should not expect it.

17. Prohibited Website.

a. The Information Management Office has blocked users from accessing inappropriate websites (for example, those devoted to pornography, hate speech, online auctions, terrorist, hacker, online personals, money-making schemes). The Savannah District's telecommunications network is intended primarily to support the Corps' mission; personal use of Government computers hinders that support by overburdening the system. The LAN sometimes has a hard enough time as it is handling all authorized data, without having to accommodate personal web surfing.

b. If you want access to a blocked website, you may request access by calling the IASO, Kerry Taylor, 652-5861. Be prepared to fully justify your request. When contacting the IASO, give the uniform resource locator (URL) of the blocked website. The IASO will view the site and determine whether to leave it blocked or to unblock it. If you disagree with the IASO's decision, you may appeal through your chain of command.

18. User Agreement. Appendix A is an agreement between you and the U.S. Government concerning use of Government computers. You will need to sign the Computer-User agreement before being issued a password. Your signature acknowledges your understanding of and agreement to support Army and Savannah District policy on the use of Government computers.

19. U.S. Army Corps of Engineers, Savannah District Computer-User Security Self-Assessment Test.

Now that you have read the guide, you may want to take the U.S. Army Corps of Engineers, Savannah District Computer-User Self-Assessment Test. To do so, log onto the Information Assurance Computer-User Self-Assessment Test Web-page at http://sasntwebrd/security/securitytest.html.

20. Conclusion.

a. As a U.S. Army Corps of Engineers, Savannah District computer user, you play a key role in protecting the integrity, availability, and confidentiality of the District's data. To recap: (1) Guard your password, (2) Follow the rules on personal use of your computer, (3) Never forward chain mail or computer hoaxes, (4) Keep your antivirus software current and running, (5) Report viruses and all other network-security incidents to your IASO.

b. Taking the steps listed above will help you ensure that your computer and all networks to which your computer is connected are safe. In doing so, you will not only be protecting yourself, you will be protecting the entire command.

# APPENDIX A

## COMPUTER-USER AGREEMENT

This appendix is a copy of the U.S. Army Corps of Engineers, Savannah District's Computer-User Agreement. Additional information is contained in the DOD 5500.7-R2301, AR 380-19, Joint Ethics Regulations, AR 380-53, and select DA messages and other applicable doctrine. URL links to these documents can be found at Appendix B. Your UPASS Administrator or Information Systems Assurance Officer will ask you to sign a copy of this agreement before issuing you a password.

As a user of the U.S. Army Corps of Engineers, Savannah District, I will adhere to the following security rules:

1. The Commander has overall responsibility for computer and network operations and security. As such, the Information Assurance Officer (IASO) is appointed to assist in the administration and enforcement of Information System Security. Questions should be referred to IASO, IAM, System Administrator (SA) or Universal Password (UPASS) Administrator.

2. I will not divulge my password to others, as I may be held accountable for their actions. If I know that my password has been compromised, I will report it to IASO, IAM, or UPASS Administrator. I am responsible for all activity that occurs on my individual login ID once my password has been used to log on, as long as I am the sole user of the login ID, and the login ID is protected by a password that is known only to me.

3. I will not forward chain mail or virus warnings. I will report chain mail or virus warnings to my IASO and delete the message. I will not attempt to run "sniffer" or other hacker-related software on the system.

4. I know I am subject to disciplinary action for any abuse of access privileges.

5. I will immediately notify to the IASO if I observe anything which may indicate inadequate security. I know what constitutes a security incident and know that I must immediately report such incidents to the IASO.

6. I will comply with security guidance issued by the IASO.

I understand this agreement and will keep the system secure. If I am the section supervisor, division chief, SA, or IASO, I will ensure that all users in my area of responsibility sign this agreement.

Name (printed): ______________________________
Signature: ______________________________ Date signed:_____________________

# APPENDIX B

## QUESTIONS FOR COMPUTER USER SECURITY TRAINING
## SELF-ASSESSMENT TEST

1. The security of our network is only as strong as the weakest link.
___ True ____ False

2. The anti-virus software should be running when you are on the computer.
___ True ____ False

3. You should open suspicious e-mail attachments.
___ True ____ False

4. An e-mail request to forward a warning to others is often an indication that the warning is a hoax.
___ True ____ False

5. AR 380-19 requires all passwords contain a minimum of how many alphanumeric characters?
____ none ____ eight ____ six

6. You are allowed to share your passwords.
____ True ____ False

7. Your use of your Government computer constitutes consent to monitoring.
____ True ____ False

8. If you notice any suspicious activity on your government computer, you should notify:
____ IASO ____ TASO ____ LASSO

9. All software on Government computers should be licensed.
____ True ____ False

10. Are you authorized to access pornography web sites?
____ Yes ____ No

11. The most common means of spreading a virus today is:
____ E-mail ____ UPS ____ CD-ROMs

12. You are responsible for any activity that takes place on a computer under your logon ID and password.
____ True ____ False

13. In order to obtain a logon ID and password, you must read and sign the Computer User Agreement.
____ True ____ False

14. You are authorized to write down your passwords or allow them to be visible to others.
____ True ____ False

15. Who should you contact if you want to load private software on your Government computer?
____ IASO ____ MISO ____ HISO

16. Should you disconnect your computer from the network?
____Yes ____ No

17. Can you install and use your own hardware at work?
____Yes ____ No

18. Who is Savannah District's IASO?
____ Kerry Taylor ____ Gary Seibert ____ Glen DePue

19. Can you load Shareware on Government computers?
____Yes ____ No

20. Should the password screen saver be activated if you are away from your computer?
____ Yes ____ No

# APPENDIX C

## Website Links and Point of Contacts

WEB PAGE FOR PUBLICATIONS LISTED IN GUIDE:

http://www.usapa.army.mil/

POINT OF CONTACTS:

| | |
|---|---|
| Help Desk | 912-652-5946 |

Information Assurance Manager (IAM):

| | | |
|---|---|---|
| Gary Seibert | 912-652-5147 | District |

Information Assurance Security Officer (IASO):

| | | |
|---|---|---|
| Kerry Taylor | 912-652-5861 | District |

Information Assurance Security Officer (IASO):

| | | |
|---|---|---|
| Jack Cox | 912-652-5309 | UPASS Administrator (CEFMS) |
| Nikisha Weston | 912-652-5360 | UPASS Administrator (CEFMS) |
| Fred Blackburn | 912-652-5547 | Engineering Division (ENCADD) |
| Stan Simpson | 912-652-5501 | Engineering Division (Water Control) |

Systems Administrator (SA):

| | | |
|---|---|---|
| Dan King | 912-652-6166 | Engineering Division (ENCADD) |
| Len Day | 912-652-6041 | District (CESAS Domain) |
| Todd McGuiness | 912-652-6159 | District (CESAS Domain) |
| Jan Constantini | 912-652-5146 | Operations Division (OP - RAMS) |
| Tanya Mercer | 706-856-0324 | Hartwell & RBR (Operations Division) |
| Nick Mosher | 706-213-3431 | Russell (Operations Division) |
| June Schulte | 864-333-1174 | Thurmond (Operations Division) |
| Steve Adair | 910-396-1211 | Construction Division (field sites) |
| David Keener | 404-464-3830 | Construction Division (field sites) |